Seamless Authentication Across Wireless Networks

Nikhil M. Deshpande, Ph.D.
Sr. Technical Marketing Engineer
Corporate Technology Group

(Rev 1, 06-13-2002)

Intel Labs

Acknowledgements

The author would like to thank Jose Puthenkulam and Abhay Dharmadhikari, Senior Software Engineer, Intel Corporation, for reviewing and providing valuable comments and suggestions to this paper.

The Wireless World Is Almost Here

Today we are at the forefront of a truly connected and wireless world. It is possible to go almost anywhere and still remain in-touch with personal and professional contacts. However, both users and service providers have needs that are not yet realized. Mobile users want fast Internet access and seamless roaming capability, without the complexities of configuring devices, inputting authentication parameters, entering and changing user preferences, updating phone books, and receiving bills from multiple service operators.

Service providers, on the other hand, need new sources of revenue. Until now, new wireless revenue has come from expanded coverage and a growing subscriber base. However, voice-based service has become a commodity as competition has increased, with the result that the average revenue per user is now falling. This revenue source has passed its maximum growth stage and cannot provide sufficient revenue to pay for the enormous cost of building infrastructure and securing spectrum for 3G services. 3G technology will provide the opportunity for new applications to be developed that will provide a new source of revenue for service providers.

Fortunately, users' demand for new services featuring seamless roaming and hassle-free authentication and configuration is converging nicely with service providers' need for new revenues. New revenue will come from new services. These new services, however, need new technologies that simplify device configuration and authentication in order to make seamless roaming possible.

The Ideal Model for Wireless Roaming

Intel envisions a usage model for wireless devices that allows one to roam at will among different networks, using whatever wireless device is currently at hand. Thus GPRS (General Packet Radio Service)-enabled cell phones, PDAs, and laptops will be able to roam and communicate freely and access the Internet across both WLANs (today mostly confined to laptops and desktops) and WWANs (today mostly confined to cell phones and pagers). The task of managing authentication between client devices and networks, often involving multiple login names and passwords, will become automatic and invisible to the user, as will the configuration of various settings and preferences that accumulate with client devices.

This is a highly desirable and lofty goal, but much work remains to make this a reality. Technology needs to move forward in multiple areas, including IP address management (incorporating mechanisms such as Mobile IP), billing management, services that roam, radio technology, and security. This paper addresses the most important aspect of security, authentication. Discussion will be further confined to authentication on GSM networks only.

As users hop freely from one network to another and from one device to another, mechanisms must be in place to continually manage authentication. "Am I who I say I am?" "Are you who you say you are?" How will user authentication be achieved in a seamless and invisible manner while roaming across multiple networks using different service providers and various wireless devices?

Where We Stand Today

Today there are a collection of standards for WLANs (of which IEEE 802.11 is the most popular) and a collection of standards for WWANs (which include GSM/GPRS, CDMA2000 1XRTT, CDMA2000 3XRTT, and W-CDMA). Some use different radio technologies and all use different communication protocols.

Among WLANs, IEEE 802.11 is well-established and quickly evolving. It defines multiple physical definitions in the form of different radio technologies operating at different frequencies and using different modulation schemes. But, for the most part, it defines a standard protocol used by all physical layers, though the protocol itself is in a constant state of upgrade and enhancement.

Among WWANs, data-based services utilizing the transmission of IP (Internet Protocol) packets are becoming available as the industry evolves from 2G to 2.5G, and eventually to 3G technology. Here, multiple standards have different physical layer definitions as well as differing protocols.

2.5G services are being added to GSM (Global System for Mobile Communications) technology in the form of GPRS and EDGE (Enhanced Data for GSM Evolution), while CDMA (Code Division Multiple Access) technology will similarly be enhanced by 1XRTT (One Times Radio Transmission Technology, or CDMA2000 1x) to provide similar data-based services. 3G services will provide higher data rates as GPRS and EDGE evolve to WCDMA (Wideband Code Division Multiple Access), and 1xRTT evolves to 3xRTT.

GSM networks use SIM (Subscriber Identification Module) technology for authenticating across networks. SIM technology is being adopted for authentication among competing WWAN technologies, as well, and promises to serve as an authentication bridge between WLANs and WWANS. Before examining how SIM technology will be used to create seamless roaming across WLAN and WWAN networks in the future, it is worthwhile to review current authentication methods for WLANs and WWANs.

Authenticating Users on WLANs and WWANs

WLANs and WWANs use different authentication mechanisms.

WLAN authentication utilizes host input and a RADIUS server

WLAN users must configure their client host (laptop or desktop) with various information including usernames and passwords, as well as network-specific parameters. The WLAN client or radio, which resides in the host, in turn uses this information to communicate via an access point with a server running an upper-layer authentication protocol, usually RADIUS (Remote Authentication Dial-In Server). If it is determined that the client is authorized on that network, then a shared key enabling secure communication is sent to the station, and network traffic is allowed to flow. IEEE 802.1X

standardizes this process by utilizing EAP (Extensible Authentication Protocol) to facilitate the authenticating mechanism (such as RADIUS) utilized by the authenticating server.

GSM WWAN authentication utilizes SIM and the switching network

A GSM mobile phone, on the other hand, contains a physical module in the form of a SIM. The SIM contains an embedded processor with its own operating system and protected memory. It contains subscriber information and algorithms for authenticating with the cellular network. It is removable and is often in the form of a miniature Smartcard. Thus a mobile professional can remove his SIM when traveling to a different country and insert it into a cellular phone that is compatible with the network in that particular country.

The mobile station (usually a phone) communicates with the network switching system via the cellular base system. If a roaming contract is found to exist for the SIM then the mobile station will be authenticated.

Enabling the Vision – SIM as a Means for Authentication

The first efforts at expanding the use of SIMs beyond WWANs are now being seen in the industry in the form of various schemes for providing GSM-like services to the customers of WLAN operators. This allows a WLAN user to access commercial WLANs in hotels and airports and use a SIM card for authentication and to manage billing. In this scenario the user simply inserts the SIM into a dongle which connects to the USB port of a laptop.

Smartcards are perceived to be very secure. In addition, all user settings and preferences can be stored on the SIM, making phone books and personal preferences portable across handsets. SIMs are an ideal means for automatic and invisible authentication and setup of personal client devices and so hold great promise for use in roaming across networks**.**

A Scenario for Getting to the Vision

Intel envisions an evolution to the ideal roaming model based on the use of SIM technology for authentication.

Short Term - Basic roaming using dongles + SIMs

Today, Intel, through collaboration with third-party companies, provides a means for automatic authentication on WLANs using a USB dongle containing a SIM Smartcard. This capability will soon be extended to allow a laptop to roam freely between GSM/GPRS WWAN networks and 802.11 WLAN networks. Users will be able to access the Internet when within range of a cellular network via GSM/GPRS radio technology, and they can take advantage of the higher bandwidth of a WLAN when they are within range of a WLAN network. The SIM card will reside on a dongle which can be plugged into the laptop.

The SIM will provide for authentication in the usual fashion when connected to a WWAN network. Authentication occurs with the WWAN switching network, using the air interface to the cellular base station.

Authentication on the 802.11 network also proceeds in the usual fashion, either through a proprietary process or through IEEE 802.1x. In this case, however, all user information is provided by the SIM, instead of the information stored in the laptop that is utilized by the NIC for traditional 802.11 network registration.

Long Term - Basic roaming using virtual SIMs

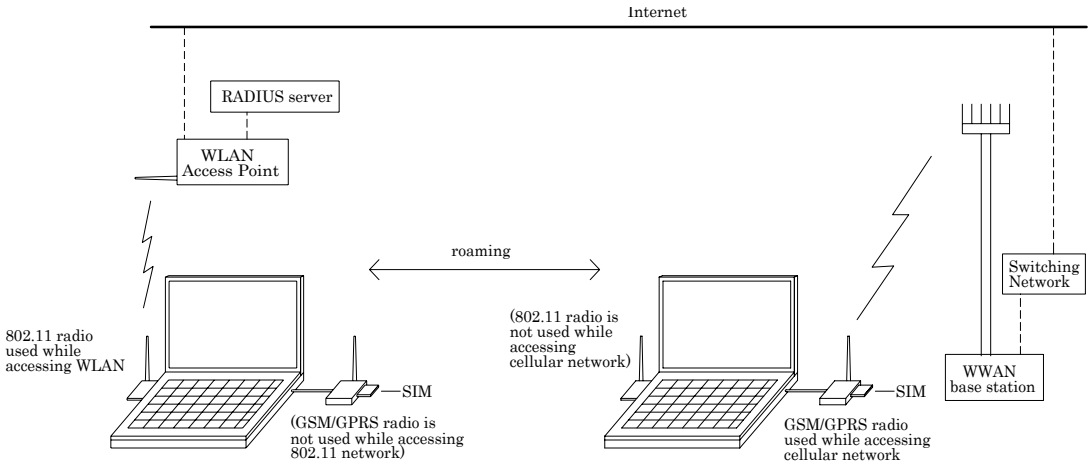
Eventually the concept of a software-based SIM can be envisioned. This provides additional flexibility for the user, while having minimal, if any, impact on back-end servers. SIMs can be stored entirely in software, thus eliminating the use of a dongle to hold a SIM card. There are many benefits to making the SIM virtual. The user no longer has to worry about keeping track of a physical card. The hassles (such as cover and battery removal) often associated with removal and insertion of SIM cards are eliminated. New devices can be configured with the user's SIM information, simply by loading the SIM into software.

The concept of a virtual SIM must be implemented in a robust and secure manner. It must provide security equivalent to a Smartcard. Authentication must take place in protected memory space that is inaccessible to outside snooping. Authentication and encryption protocols must be carefully designed to properly use standard public security algorithms that have been time-tested by the industry.

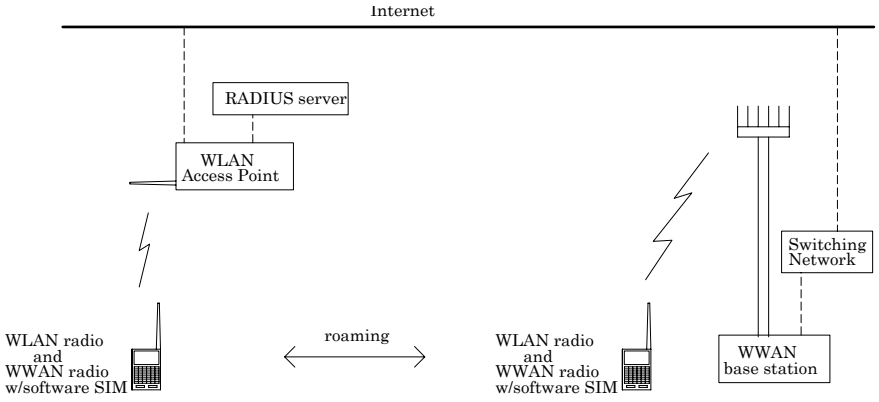
Use of Bluetooth to transfer SIMs between client devices*

Ultimately, by taking advantage of Bluetooth* functionality to allow invisible and automatic location of services, a personal client could locate a virtual SIM, and borrow it (with permission) from another device. A Bluetooth-enabled device can communicate with other Bluetooth-enabled devices over a small WPAN* (Wireless Personal Area Network). Bluetooth networks form automatically when enabled devices are in close proximity to one another, enabling discovery of services and sharing of information.

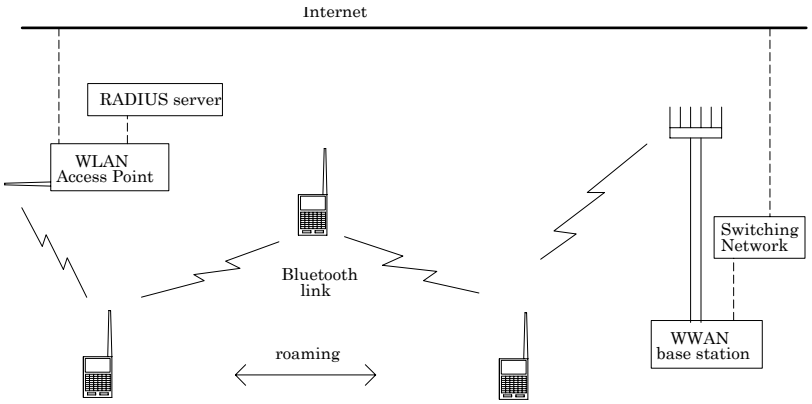
Now the user can buy a new cell phone or PDA and not have to worry about programming SIM information. If a device is lost or stolen, the SIM information and any additional personal information such as phone book entries can be easily recovered simply by obtaining it from another device which contained the same information. Once SIM information has been located and loaded via a Bluetooth transaction, all authentication and billing information, user preferences, etc. will be immediately available to the device. To ensure that a lost or stolen SIM is not used in a fraudulent manner, it will be necessary to incorporate a mechanism to disable the virtual SIM in a missing device.



Short term – Laptop equipped with GPRS and 802.11 radios can roam between WLAN and WWAN. It authenticates on both networks using subscriber information stored on the SIM card in the GPRS radio.



Long term – Personal Internet Clients with built-in radios can roam between WLAN and WWAN and authenticates using subscriber information stored in virtual SIM in software.



Addition of Bluetooth – All devices contain software radios which can be configured for WLANs, WWANs, and WPANs. A Bluetooth WPAN can be used to locate and borrow (with permission) a virtual SIM from another device.

Figure 1 –Authentication While Roaming Between WLANs and WWANs

Intel PCA – Making it Happen

Intel PCA (Personal Internet Client Architecture), which separates communication tasks and processes from application processing, will enable rapid innovation of new applications for seamless roaming. Intel is making standard building blocks and APIs for both server and client hardware available as part of the PCA Development Kit. Developers can use future building blocks to implement tasks involving roaming and virtual SIMs. By allowing developers to roam and authenticate using SIMs, the door is opened for a world of new, as of yet, unimagined applications and services.

Developing with Intel PCA has many far-reaching benefits. By separating hardware development from software development and allowing them to proceed independently and in parallel, Intel PCA allows application development to proceed at a much faster pace. Applications developed with Intel PCA will maintain compatibility with legacy equipment, while being assured of compatibility with future equipment. In addition, all applications will benefit from Intel's commitment to make quality-of-service paramount in fulfilling user expectations for applications and services.

Intel PCA will enable developers to dream of next-generation wireless applications without worrying about incompatibility issues when users move from device to device, and from network to network. Intel PCA-compatible applications that utilize virtual SIMs will utilize roaming and discovery of services to provide users new and exciting capabilities. These new applications will generate new growth opportunities for wireless providers and satisfy users' desires for convenience, security, and freedom in today's wireless world.